

# Avoiding AML/BSA enforcement actions



## Regulatory

# Avoiding BSA/AML enforcement actions

by Edward Monahan

Last year, regulators imposed collectively more than 20 formal enforcement actions as well as a multitude of informal agreements on banks relating to BSA/AML deficiencies.

In 2004 and 2005, the evolution of Bank Secrecy Act/Anti-Money Laundering (“BSA/AML”) risk management standards was accelerated by an unprecedented number of high profile Bank Secrecy Act/Anti-Money Laundering (“BSA/AML”) regulatory enforcement actions. Last year, regulators imposed collectively more than 20 formal enforcement actions as well as a multitude of informal agreements on banks relating to BSA/AML deficiencies. These actions emphasized regulators’ views that internal controls for preventing money laundering and terrorist finance are a cornerstone of corporate governance as well as an indicator of enterprise-wide risk management integrity. The scope and intensity of regulatory consent orders and associated monetary fines were unprecedented.

Two prominent cases illustrate the perils of BSA/AML non-compliance: 1) AmSouth paid \$54 million in fines stemming from agreements with the Federal Reserve and FinCEN as well as a deferred prosecution agreement with the U.S. Department of Justice;<sup>1</sup> and, 2) Riggs National Bank paid \$51.7 million for BSA violations incurred at its international private banking and Embassy Banking business divisions.<sup>2</sup> At the same time, both banks have sustained huge costs for corrective programs and remedial management: AmSouth plans to spend \$9 million annually to fix BSA/AML problems<sup>3</sup> while Riggs National Bank absorbed \$73 million in overall costs to fix deficient processes and close troubled operations.<sup>4</sup> BSA/AML enforcement-related sanctions obligated Riggs National Bank to shut down key business lines and replace senior management. Thereafter, in May of 2005, the Riggs National Board sold Riggs Bank to Pittsburg National Corporation. In an overall sense, BSA/AML risk management has become the costliest area of compliance for U.S. banks: industry forecasts suggest that institutions will have spent more than \$11 billion on AML pro-

gram development, consulting assistance, software and training from 2002 to 2005.<sup>5</sup>

The financial services industry has observed these developments with a mixture of fear and loathing. A public enforcement action causes reputational damage, and remedial management costs cripple an institution’s strategic expansion and operating effectiveness. Until recently, BSA/AML regulatory enforcement has generally lagged behind evolving technologies, global financial infrastructures and instantaneous communications. However, recent federal and state enforcement scope has hardened: the severity of BSA/AML enforcement actions by the four federal regulators<sup>6</sup> is without precedent, as is the criminalization of violations that had been historically treated as civil regulatory matters.

Regulatory expectations for banks center around the requirement that BSA/AML compliance be based upon a written, Board-approved BSA/AML program<sup>7</sup> comprised of four elements:

- 1) Internal Controls supporting compliance with BSA regulations;

<sup>1</sup> AmSouth Bancorporation, S.E.C. Form 10-Q, Management’s Discussion and Analysis of Financial Condition and Results of Operations as of 9/30/04— Third Quarter and First Nine Months Overview, page 20.

<sup>2</sup> Riggs National Corporation, S.E.C. Form 10-K, Item 7: Management’s Discussion and Analysis of Financial Condition and Results of Operations as of 12/31/04 – Item 7A: Quantitative and Qualitative Disclosures About Market Risk, page 30. Fines were: a) \$25.0 million from the OCC and the Financial Crimes Enforcement Network in the second quarter of 2004; b) \$16 million from the United States Department of Justice recorded in the fourth quarter of 2004; c) \$8 million accrual for fourth quarter of 2004 related to litigation in Spain; and, d) \$2.7 million for settlement of stockholder litigation.

<sup>3</sup> AmSouth Bancorporation, S.E.C. Form 10-Q, under section entitled Third Quarter Settlements, page 20.

<sup>4</sup> Riggs National Corporation, S.E.C. Form 10-K, as above, at page 30.

- 2) Independent testing performed by internal auditors or staff;
- 3) Designated Compliance Officer responsible for day-to-day oversight; and,
- 4) Training of staff involved with areas relevant to BSA/AML compliance.

This program must allow banks to:

- Know their customers;
- Report large cash transactions;
- Identify suspicious activities;
- Maintain systems and processes equal to the risks of relationships, products and activities; and,
- Forestall terrorist finance and money laundering through cooperation with law enforcement and regulators.

Comprehensive regulatory expectations have been spelled out clearly by the Federal Reserve and the OCC. The Federal Reserve has declared that “financial institutions are expected to have a sound anti-money laundering compliance program...(that)...must include well-defined processes to identify suspicious activities, and those processes should be tailored to the risk and complexity of each business line.”<sup>8</sup> Further, the OCC has offered an extraordinary and blunt declaration of principle regarding the rise in enforcement actions and penalties. It serves as a warning to

bank managements and compliance officers: “Unlike other examination areas, a statutory mandate exists that instructs the OCC to issue a cease-and-desist order (C&D) whenever a bank fails to establish and maintain a BSA compliance program....”<sup>9</sup> The OCC’s Chief Counsel has added “...what was good enough in the past may not be good enough now...”<sup>10</sup>

Based upon a careful reading of recent Written Agreements, Memoranda of Understanding and Cease & Desist Orders,<sup>11</sup> banks should prepare for expanded scope BSA/AML examinations by focusing on the following key internal control issues:

- 1) **Management oversight:** Examiners will assess a bank management’s commitment to BSA/AML compliance by evaluating whether internal controls are supported by sound procedures, independent audit testing, competent compliance staffing and effective employee training. Such regulatory actions also emphasize that the business unit, rather than the compliance department, must assume responsibility for maintaining compliance and monitoring customer behavior.
- 2) **Suspicious activities:** Examiners want to be assured that a bank can distinguish between customary activities and unusual transactions, and that a process exists to investigate, analyze and articulate reasonable SAR filing decisions based upon credible infor-

mation. Examiners will probe information technology systems and back-end analytical departments in hopes of finding a sound case management process that is supported by reasonable financial intelligence. Indeed, while certain businesses and activities may demand more intensive customer due diligence because of their inherent BSA/AML risk (e.g., private banking versus retail consumer deposit-taking), bankers will be punished severely for complacency or inaction. BSA/AML control standards are rising across all areas of financial institution activity. Excessive defensive filings may indicate that a bank does not know how to distinguish between questionable activities and legitimate customer behavior.

- 3) **Customer risk rating:** Examiners will consider a bank to be a “high-risk institution” if it is inattentive to a need for automated systems, internal controls and testing. Sophisticated recordkeeping and monitoring systems are very expensive to acquire, implement and maintain. Therefore, financial institutions should plan and budget aggressively for major upgrades over the next few years as BSA/AML risk management software continues to evolve. These resources support comprehensive ranking of risks aligned with customers, products and activities. Banks that deploy sound internal controls while operating in high-risk jurisdictions and offering high-risk products will meet regulatory standards; those operating

<sup>5</sup> Article entitled “Banks Taken to Cleaners in Terrorist Search” by Tomas Kellner, Forbes, May 14, 2004.

<sup>6</sup> Office of the Comptroller of the Currency (OCC), Federal Reserve Bank, Office of Thrift Supervision and Federal Deposit Insurance Corporation.

<sup>7</sup> Patriot Act Section 352 and 12 CFR 21.21(c).

<sup>8</sup> Remarks by Federal Reserve Bank Governor Bies to the Institute of International Bankers, March 14, 2005.

<sup>9</sup> OCC Bulletin 2004-50: Enforcement Guidance for BSA/AML Program Deficiencies, November 10, 2004.

<sup>10</sup> Remarks of OCC Acting Chief Counsel Stipano to Florida International Bankers Association, February 10, 2005.

<sup>11</sup> Publicly released enforcement documents such as: Riggs National Bank, AmSouth, Banco Popular, ABN Amro, Standard Chartered, Banco de Chile, HSBC, Western Union, Eagle National Bank of Miami and Hudson United Bank.

## Regulatory

in lower-risk areas with standard products and services will fail examinations if they view controls as an unnecessary cost rather than a critical necessity.

- 4) **Policies & procedures:** Examiners believe that Patriot Act requirements for Customer Identification Programs (that support Know-Your-Customer capabilities) should be implemented and operative, because such CIP regulations and rules were finalized long ago. Examiners will inspect a bank's BSA/AML Program for completeness and effectiveness. They expect to find evidence that accurate and prompt regulatory reporting, suspicious activity and OFAC monitoring, compliance oversight, due diligence review capabilities and employee training are operative and effective.

Lack of a sound BSA/AML Program or failure to execute remedial measures for

correcting unfavorable examination findings will provoke issuance of an enforcement order that typically carries aggressive timelines for fixing deficiencies. Weak BSA/AML Programs may need to be strengthened within 60 days. Reporting failures may lead to a requirement to reexamine historical transaction data over a previous one- to three-year period. This is a complex, costly and burdensome undertaking that requires banks to gather and upload historical data into a separate server in order to filter transactions against enhanced suspicious activity detection criteria. These tasks must often be accomplished within 180 days. During this "look-back" project period, with a bank under an enforcement order, strategic initiatives and growth plans may be prohibited by regulators.

[Banks ought to adopt a proactive, anticipatory approach to regulatory risk management by preparing for outside](#)

[scrutiny and identifying deficiencies before regulatory examinations uncover major problems.](#) Management or Internal Audit should perform detailed analyses of customer files, monitoring programs, staffing levels, BSA/AML procedures, controls and information systems in order to provide senior management with cost estimates and timeframes for pre-exam remedial actions. Given the nature of money laundering and terrorist finance, the most important BSA/AML regulatory expectation relates to action-oriented management: do not wait for examiners to find problems. Bank management should identify customers, contain risks and implement solutions before they are "ordered" to do so.

For more information on Avoiding BSA/AML Enforcement Actions, please contact Edward Monahan at 617.530.6398 or [edward.monahan@us.pwc.com](mailto:edward.monahan@us.pwc.com).

Previous successful regulatory examinations offer no assurance that new or current BSA/AML scrutiny will be lenient. Indeed, complacency may lead to sanctions and fines. Prudent bank management should aggressively inspect the sufficiency of BSA/AML programs in order to assess these issues:

- Has the bank evaluated its BSA/AML risks? Is the program tailored to specific identified risks? If the risk assessment was completed by an internal department or an external consultant, have I analyzed and agreed to its conclusions? Does the analysis target all relevant specific business risks?
- Do the conclusions of the last examination report relate to embedded BSA/AML issues that have not been addressed? Current outstanding issues or problems often turn into next year's regulatory enforcement action.
- Do officers and staff understand the severity of BSA/AML risks and the consequences of inaction to the financial institution both today and tomorrow?
- Is the bank's BSA/AML audit testing program and, indeed, the internal auditors themselves, sufficiently strong to identify and act promptly on problems that may have been missed or problem customers that the bank may have failed to identify?